

Serial No. 10/089,905
Internal Docket No. RCA 89865

Remarks/Arguments

Claims 1-3, 5-9 and 12-22 stand rejected pursuant to 35 U.S.C. 102(e) as being anticipated by Graunke (United States Patent No. 6,731,758). Claims 1, 5, 13, 17, 19 and 21 have been amended to more clearly and distinctly claim the subject matter that applicants regard as their invention. Applicants traverse and respectfully request reconsideration and removal of these rejections for at least the following reasons.

A claim is anticipated pursuant to 35 U.S.C. 102 only if each and every element set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *See, Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)*). In other words, in order for a prior art reference to anticipate a claim, "the identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)*: And, each of the claim elements must be arranged as required by the claim. *See, In re Bond, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990)*.

Turning to Claim 1, it recites, in its entirety:

A method for verifying that a source device that is capable of receiving protected content is authorized to communicate the protected content to a sink device that is capable of descrambling the protected content comprising:

receiving at said source device an approval code associated with said source and sink devices;

determining, in said source device, a local code using data associated with said source and sink devices; and

comparing, in said source device, at least a portion of said approval code to at least a portion of said local code, **verifying that the sink device is authorized to receive the protected content from said source device in response to the comparison, and providing access to the protected content to the sink device in response to the verifying step.** (emphasis added)

Thus, in order to anticipate Claim 1, Graunke must at least: (1) compare, in the source device, at least a portion of a source device received approval code to at least a portion of a source device determined local code; (2) verify that the sink device is authorized to receive the protected content from said source device in response to the comparison; and (3) provide

Serial No. 10/089,905
Internal Docket No. RCA 89865

access to the protected content to the sink device in response to the verifying step. However, Graunke fails to teach the above-identified steps, and hence fails to anticipate Claim 1.

The teachings of Graunke have been discussed in detail in applicants' responses dated April 27, 2006, and September 22, 2006. As detailed in those responses, applicants submit that Graunke fails to teach or suggest the above mentioned features, but rather discloses an authentication process for authenticating the identify of the devices (col. 3, lines 1-31) and a verification process for confirming that content is being properly deciphered by the receiver (col. 3, lines 32-55). However, nowhere does Graunke teach or suggest steps related to authorization as recited in the pending claims.

In response, the examiner states "... the case law disclosed in final rejection recognizes that if a process is being disclosed in the prior art, then such process is not novel nor an inventive step, and as far as applicant's arguments are concern[ed] the limitation of the comparison of the codes or values for verification or authentication is prior art regardless of the claim language. It is the steps of such authentication that may have a novelty or an inventive steps, NOT the broad limitation of comparison and authentication based on two value. (emphasis in original)"

Applicants particularly disagree with examiner's assertion that the "... the limitation of the comparison of the codes or values for verification or authentication is prior art **regardless of the claim language...**(emphasis added)" The claim language defines the invention and are **chosen for their particular meaning**, and distinguish over the teachings of Graunke. In this case, the claims are directed to a method for verifying authorization to communicate protected content and the claim language reflects such subject matter, not to a verification or authentication process.

As is well known by those skilled in the art, authentication and authorization are separate and distinct concepts. See for example, the description of authentication and authorization in the attached web page <http://www.belluelinux.org/authentication.html> published by The Linux Information Project. As described in the web page, authentication refers to a process of confirming the identity of a person that is attempting to access a system, while authorization refers to the process of giving individuals access to a system objects based on their identity. Authentication confirms the identity of the entity, but says nothing about the access rights of that entity. As such, successful authentication does not

Serial No. 10/089,905
Internal Docket No. RCA 89865

necessarily result in an entity having access to protected content. Authorization is performed to determine the access rights of that entity. In view of the above, applicants submit that the claim language is, in fact, particularly relevant in distinguishing the subject matter of the claims from the teachings of Graunke.

Applicants also submit that verification of proper deciphering as described in Graunke is separate and distinct from the verifying of authorization as recited in the claims. Authorization, as mentioned above, relates to determining access rights to particular content by a particular entity. Verification as described in Graunke is unrelated to such access rights determination. Rather, the verification of Graunke relates to confirming that a receiver is properly deciphering the content. Clearly, the matter of whether the receiver is entitled to receive the content is unrelated to whether the deciphering is properly performed by the receiver as discussed in Graunke. In view of the above, applicants respectfully disagree that the claimed process is not disclosed in Graunke as alleged.

Further, applicants respectfully disagree with the assertion that "It is the steps of such authentication that may have a novelty or an inventive steps, NOT the broad limitation of comparison and authentication based on two value. Again, applicants submit that authentication and authorization are separate and distinct concepts, and are not same concepts as the examiner appears to allege. Finally, applicants note that, for example, Claim 1 does not merely recite a broad limitation of comparison and authentication based on two values as alleged. Rather, the claims recite specific steps of, for example, in claim 1, receiving and approval code associated with source and sink devices, and determining a local code using data associated with the source and sink devices, as well as the comparing and verifying steps. These steps are not disclosed or suggested in Graunke. Claims 5, 13, 17, 19 and 21 similarly are directed to verifying whether a particular device is authorized to receive protected content.

In view of the foregoing, applicants submit that present claims 1-22 are not anticipated by Graunke. However, to move the prosecution of this case forward, applicants have further amended the claim to clarify the difference between the present invention and the teachings of Graunke. In particular, the claims have been amended to recite verifying that the sink device is authorized to receive the protected content from the source device in

Serial No. 10/089,905
Internal Docket No. RCA 89865

response to the comparison, and providing access to the protected content to the sink device in response to the verifying step. In this manner, the present claims clearly distinguish from the teachings of Graunke as they relate to authentication and verification of proper deciphering.

As mentioned above, authentication relates to confirming the identity of a particular entity, not the access rights. Graunke says nothing in regard to performing authentication to determine the access rights to particular content by a particular entity. Thus, this aspect of Graunke fails to disclose or suggest providing access in response to the verifying step as recited. Also, the verification of proper deciphering relates to confirming that the receiver is properly deciphering the transmitted content. This process is also unrelated to determining whether a particular entity is entitled to access the content. In fact, authorization is moot in such verification because the receiver is already receiving the content. The question addressed by the verification is whether the receiver is properly deciphering the content, not whether the receiver is entitled to receive the content. Thus, this aspect of Graunke also fails to disclose or suggest providing access in response to the verifying step as recited.

Claims 5, 13, 17, 19 and 21 have been amended in similar fashion and are believed to be not anticipated by Graunke for at least the same reasons as those discussed above with respect to claim 1.

As to the rejection of claims 4, 10, and 11 under 35 USC 103(a) as being unpatentable over Graunke, applicants submit that the additional teachings that are alleged to be well known fail to cure the defect of Graunke as applied to claims 1 and 5. Therefore, applicants submit that claims 4, 10 and 11, which depend from claims 1 and 5, are also patentably distinguishable over the teachings of Graunke for at least the same reasons as those discussed above with respect to their base claims.

Serial No. 10/089,905
Internal Docket No. RCA 89865

CONCLUSION

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,

DAVID J. DUFFIELD et al.

By: 
Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: November 7, 2006

LINFO

Authentication Definition

Authentication is the process of confirming the identity of a person that is attempting to access a system or of confirming the *authenticity* of a message.

Authentication is distinct from *authorization*, which is the process of giving individuals access to system objects based on their identity. Authentication merely confirms the identity of the individual, but says nothing about its access rights. Authenticity refers to whether both the source and the content of a message are what they are claimed to be.

Authentication can be based on something that a person knows, has or is. Examples of the first include user names, passwords and pass phrases. Examples of the second include IP addresses, digital signatures, cell phones and identification cards. The third consists of biometric data, which includes fingerprints, palm patterns, iris scans, voice recognition and facial recognition.

A *digital signature* is a method for authenticating digital information which is implemented using techniques from public key cryptography (PKC). It usually involves two complementary algorithms, one used for signing and the other used for verification.

None of these methods are completely secure, and all could be vulnerable to *spoofing*, i.e., pretending to be someone or something else. For example, there are ways of discovering user names and passwords, IP addresses can be forged, and even fingerprints can be falsified (such as by using a thin layer of a transparent material that contains someone else's fingerprints).

The chances of successful break-ins can be greatly reduced by requiring multiple types of authentication. And authorization helps minimize the compromising of data or other damage in the event of a break-in.

A major feature of Linux and other Unix-like operating systems is that they can be extremely secure when used according to standard security guidelines (e.g., requiring strong passwords, utilizing the root account only when necessary, shutting down unnecessary services, using a strong firewall and providing physical security). Among the ways in which they accomplish this is by combining authentication (i.e., the requirement for a user name and password in order to log into the system) with a fine-grained system of authorization, referred to as *permissions* (i.e., *read*, *write* and *execute* permissions that can be set individually for every file, directory or other object on the system).

Authentication has been a crucial factor in the success of networks, ranging from local area networks (LANs) to the Internet.